DEPARTMENT OF THE NAVY
BUREAU OF NAVAL PERSONNEL
5720 INTEGRITY DRIVE
MILLINGTON, TN 38055-0000

Canc frp: Oct 11

BUPERSNOTE 5239
BUPERS-073
12 NOV 2010

BUPERS NOTICE 5239

From: Chief of Naval Personnel

Subj: BUREAU OF NAVAL PERSONNEL POLICY STATEMENT ON SAFEGUARDING PERSONALLY IDENTIFIABLE INFORMATION (PII)

Ref: (a) Privacy Act of 1974
(b) DON CIO WASHINGTON DC 091256Z Oct 2007
(c) SECNAV WASHINGTON DC 232026Z Jul 2007
(d) DON CIO WASHINGTON DC 291652Z FEB 2008
(e) DRMSINST 4160.14 of 12 May 2008
(f) BUPERSINST 5211.6
(g) SECNAVINST 5239.3B

Encl: (1) Chief of Naval Personnel Policy Statement on Personally Identifiable Information (PII)

1. Purpose. To promulgate the policy for the implementation of references (a) through (g), for the proper handling of personally identifiable information (PII) when stored on government furnished desktop computers, laptop computers, other mobile computing devices, and removable storage media (e.g., removable hard drives, thumb drives, blackberries, personal digital assistants, compact discs, digital video discs, etc.). The use of USB thumb drives, memory sticks/cards and camera flash cards is PROHIBITED from use on all Navy Networks until further notice. References (b), (c) and (d) are available at http://www.doncio.navy.mil. Reference (e) can be found at http://www.drms.dla.mil.

2. Background. Per reference (a), agencies are required to establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of records to protect against any anticipated threats or hazards to their security or integrity. The loss or compromise of PII can lead to identity theft, which directly impacts department personnel, contractors, retirees and their dependents. Safeguards must be

applied to information technology (IT) systems, share drives, computer networks, e-mail, paper records and Web sites to ensure the security of PII.

3. Action. All unclassified PII Data at Rest (DAR) and data in transmission that has not been approved for public release and is stored on government furnished computing devices shall be treated as sensitive data and encrypted using commercial available encryption technology as outlined in enclosure (1). Storage of any form of PII is prohibited on personally owned computing devices, i.e., desktop computers, laptop computers, mobile computing devices, and removable storage media.

4. Point of contact is Bureau of Naval Personnel, Information Management Office (BUPERS-07), (901) 874-4160/DSN 882.

5. Records Management. Records created as a result of this instruction, regardless of media and format, shall be managed per Secretary of the Navy Manual M-5210.1 of November, 2007.

6. Cancellation Contingency. This notice will remain in effect for 1 year or until superseded, whichever occurs first.

D. P. QUINN
Rear Admiral, U.S. Navy
Deputy Chief of Naval Personnel

Distribution:
Electronic only, via BUPERS Web site
http://www.npc.navy.mil/

BUPERSNOTE 5239
12 NOV 2010

CHIEF OF NAVAL PERSONNEL

POLICY STATEMENT ON LOSS PREVENTION OF PERSONALLY IDENTIFIABLE INFORMATION (PII) DATA

1. Per references (b) and (c), all unclassified DAR that has not been approved for public release and is stored on mobile computing devices shall be treated as sensitive data and encrypted using commercially available encryption technology. The Department of Defense (DoD) and Office of Management and Budget have mandated the protection of DAR on all unclassified NMCI seats/devices. Navy Marine Corps Intranet (NMCI) has implemented GuardianEdge Encryption Anywhere and Removable Storage software to meet these requirements. All data in computer storage, as well as data written to a removable storage device, will be encrypted. Any desktop computer, laptop computer, mobile computing device, or removable storage media that processes or stores a compilation of electronic records or files containing PII shall be restricted to DoD owned, leased, or occupied workplaces. When compelling operational needs require removal from the workplace, the laptop computer, mobile computing device, or removable storage media shall:

a. Be signed in and out with a supervising official designated in writing by senior leadership;

b. Be configured to require certificate-based authentication for log on;

c. Be set to implement screen lock, with a specified period of inactivity not to exceed 15 minutes;

d. Have all PII stored on, created on, or written from laptop computers, mobile computing devices, and removable storage media encrypted; and

e. Encrypt all e-mails containing PII, privacy act, and other categories of DoD sensitive information while in transit across the global information grid.

2. Storage of any form of PII is prohibited on personally owned laptop computers, mobile computing devices, and removable storage media.

3. Laptop computers and mobile computing devices and the data stored on removable storage media must be encrypted.

4. Ensure all documents containing PII are marked "For Official Use Only - Privacy Sensitive any misuse or unauthorized disclosure can result in both civil and criminal penalties."

5. While much of the turn-in process involves the Defense Reutilization and Marketing Service (DRMS), NMCI or other Department of the Navy (DON) network owners, the local command or unit is responsible for information security, physical security and property accountability for all excess Legacy unclassified equipment awaiting sanitization, shipment to DRMS or release to another DoD component or donation activity. Per reference (d), at a minimum local commands shall:

a. Remove all drawers in desks and file cabinets to ensure stray documents are removed;

b. Ensure all lockable drawers or cabinets are open for inspection;

c. Comply with ASD Memo "Disposition of Unclassified DoD Computer Hard Drives" of 4 June 2001, which provides specific instructions on how to dispose of hard drives in the DoD; http://iase.disa.mil/policy-guidance/asd hd disposition memo060401.pdf.

d. Use National Security Agency approved sanitization equipment to properly overwrite and degauss excess unclassified hard drives. Ensure verification labels are placed on all hard drives that have been degaussed and overwritten;

e. Ensure copier hard drives have been properly overwritten and degaussed;

f. Provide training for all personnel on how to accurately prepare and process excess unclassified IT equipment before forwarding to DRMS; and

g. Keep accurate destruction and turn-in records for a minimum of 5 years.

6. The local command or unit is NOT responsible for information security, physical security or property accountability for any NMCI excess unclassified equipment awaiting sanitization, shipment to DRMS or release to another DoD component or donation activity.

7. Echelon 3 Information Assurance Managers are responsible for and will provide training on the proper encryption process within specific commands.

8. ALL DON personnel (i.e., military, civilian, and contractors) must be aware of their roles and responsibilities related to reporting a known or suspected loss of PII. DON personnel who have discovered a known or suspected loss of PII must report the breach to their supervisor. Commands/activities will designate an official in the chain of command responsible for reporting PII breaches and to serve as a point of contact for follow-up actions and individual notifications. Ensure prompt and complete reporting of all PII incidents and suspected incidents per reference (e). This includes reporting whether the loss reported was encrypted, as required above.

9. Guidance and tools on implementing encryption of data are available at:

a. Data at Rest Encryption Security Computer-Based Training (https://www.homeport.navy.mil/training/security/dar/).

b. Data at Rest Encryption Security Frequently Asked Questions (https://www.homeport.navy.mil/training/security/dar/).

c. Data at Rest Encryption Security Topic Guide (https://www.homeport.navy.mil/support/articles/data-at-rest/).

10. The DON enterprise solution for protection of sensitive DAR on non-NMCI assets is now available. Implementation of this solution enables compliance with DoD and DON requirements associated with protection of PII and other types of sensitive DAR on mobile computing devices and portable storage media.

11. Additional guidance, as well as training and other privacy resources, are available on the Navy's privacy Web site at http://privacy.navy.mil.